An Improved Authentication Protocol Without Trusted Third Party*

Min-Shiang Hwang† Chin-Chen Chang‡ Kuo-Feng Hwang‡

Department of Information Management †
ChaoYang University of Technology
168, Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@mail.cyut.edu.tw
http://www.cyut.edu.tw/~mshwang/

Department of Computer Science and Information Engineering ‡
National Chung Cheng University
Chaiyi, Taiwan, R. O. C.

September 8, 2001

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-005.

†Responsible for correspondence.

An Improved Authentication Protocol Without Trusted Third Party

Abstract

This letter presents a secure authentication protocol which supports both the privacy of messages and the authenticity of the communicating parties. A scheme for extending a secure authentication protocol to improve the security of the communicating parties is also proposed.

Index Terms: Authentication, Cryptography, Security.

1 Introduction

Recently, Shieh-Yang-Sun proposed an authentication protocol without a trusted third party [1]. The protocol is based on both the ID-based scheme [2, 3] and symmetric cryptographic techniques (such as DES [4] and FEAL [5]). The protocol proposed by them is easier to implement than other authentication protocols.

Shieh-Yang-Sun stated that their protocol supports both the privacy of messages and the authenticity of the communicating parties. In this letter, it is shown that their protocol only supports the privacy of messages. The authenticity of the communicating parties is not supported by their protocol. A scheme for extending a secure authentication protocol so that the authenticity of communicating parties will be improved is also proposed.

2 The Drawbacks of Shieh-Yang-Sun's Protocol

There are two phases in Shieh-Yang-Sun's Protocol: the initial phase and the authentication phase. The initial phase is completed at the key information center for setting up the system. The main role of the key information center is to generate public and secret information for the newly registered users. After the initial phase, there are four parameters which are owned by user i: $n, g, f(\cdot)$, and S_i. Here n, g, and $f(\cdot)$ are public information, where n is a product of two large prime numbers p and q, wheer $\gcd(3,(p-1)(q-1)) = 1$. g is an integer which is a primitive element in both $GF(p)$ and $GF(q)$. S_i is a signature of user i, computed by the following equation.

$$S_i = EID_i^d \bmod n, \tag{1}$$

where d is the center's secret information which satisfies the following equation.

$$3 \cdot d \bmod (p-1)(q-1) = 1. \tag{2}$$

EID_i is the ith user's extend identity (ID_i), computed by the following equation.

$$EID_i = f(ID_i) \bmod 2^N, \tag{3}$$

where $f(\cdot)$ denotes a one-way function and N denotes the bit length of EID. Here S_i is the secret information.

The authentication phase of Shieh-Yang-Sun's protocol is executed between the two communication parties to achieve mutual authentication and exchange their common session key. If user i wishes to communicate with user j, he generates a random number r_i and computes

$$\left\{ \begin{array}{ll} X_i & = g^{3r_i} \bmod n, \\ Y_i & = S_i \cdot T_i \cdot g^{2r_i} \bmod n, \end{array} \right. \tag{4}$$

where T_i is the current time of the system. User i sends (X_i, Y_i, T_i, ID_i) to user j. Upon receipt these messages, user j checks T_i whether it was sent recently. Then the user j checks whether the following equation holds:

$$Y_i^3 = f(ID_i) \cdot T_i^3 \cdot X_i^2 \bmod n. \tag{5}$$

If the equation holds, then user j authenticates the message which was sent by user i. Thereafter, user j generates a random number r_j and executes the same procedures as that of user i.

Finally, users i and j computes the session keys K_{ij} and K_{ji}, respectively.

$$K_{ij} = X_j^{r_i} = g^{3r_jr_i} \bmod n, \tag{6}$$

$$K_{ji} = X_i^{r_j} = g^{3r_ir_j} \bmod n. \tag{7}$$

User i and user j thus use $K_{ij} = K_{ji}$ as their common secret key.

In the subject of the paper [1], the authors showed that if a forger wants to masquerade as user i to communicate with others, he must find two integers X and Y satisfying Equation (5). However, we show that a forger needs not find the two integers X and Y for satisfying Equation (5) as follows.

1. We assume that a forger intercepts four parameters: (X_i, Y_i, T_i, ID_i), which is sent by user i. These parameters can be easily obtained, since they are sent through public channels.

2. If the system's current time is T_i', the forger computes the following equation:

$$Y_i' = Y_i \cdot (T_i'/T_i) \bmod n. \tag{8}$$

The forger thus masquerades as user i to send (X_i, Y_i', T_i', ID_i) to user j.

Upon receipt of the messages: (X_i, Y_i', T_i', ID_i), user j checks whether Equation (5) holds. Since the following equation holds:

$$Y_i^{'3} = f(ID_i) \cdot T_i^{'3} \cdot X_i^2 \bmod n, \tag{9}$$

user j is thus cheated by the forger.

Therefore, Shieh-Yang-Sun's protocol does not support the authenticity of the communicating parties. Although the authors stated that the replay-attack will not succeed, T_i will be redundant in their protocol. In fact, the security is the same as that of Shieh-Yang-Sun's protocol while removing T_i from their protocol. But the protocol of removing T_i in Shieh-Yang-Sun's protocol is easier and faster to implement than their original protocol.

In the next section, we extend Shieh-Yang-Sun's protocol to support both the privacy of messages and the authenticity of communicating parties.

3 Our Improved Scheme

Shieh-Yang-Sun used the concept of timestamp to check the message legality. Since the timestamp is linear in Equation (4), a forger can masquerade as user i by computing Equation (8).

To enhance the authentication, we propose an extended scheme which is modified from Shieh-Yang-Sun's protocol. Our improved scheme is stated as follows.

1. If user i wishes to communicate with user j. He generates a random number r_i and computes X_i and Y_i as follows.

   $$\begin{cases} r_i' &= r_i \cdot T_i \bmod \lambda(n), \\ X_i &= g^{3r_i} \bmod n, \\ Y_i &= S_i \cdot g^{2r_i'} \bmod n, \end{cases} \tag{10}$$

   where, $\lambda(n) = Lcm(p-1, q-1)$.

2. User i sends the following four parameters, X_i, Y_i, T_i, and ID_i, to user j.

3. Upon receipt (X_i, Y_i, T_i, ID_i), user j checks T_i whether it was sent recently. Then the user j checks whether the following equation holds:

   $$Y_i^3 = f(ID_i) \cdot X_i^{2T_i} \bmod n. \tag{11}$$

If the equation holds, then user j authenticates the message which was sent by user i. The remaining steps are the same as that of Shieh-Yang-Sun's protocol.

Thereafter, user j generates a random number r_j and executes the same procedures as that of user i.

The timestamp is non-linear in Equation (10), a forger who wants to masquerade as user i finds it difficult to solve non-linear equations. Therefore, our extended protocol can support both the privacy of messages and the authenticity of communicating parties.

4 Conclusions

It is shown here that Shieh-Yang-Sun's protocol cannot support the authenticity of the communicating parties. An extended protocol which is a slight modification of Shieh-Yang-Sun protocol is proposed. This protocol can support both the privacy of messages and the authenticity of communicating parties. The proposed protocol not only retains all the advantages of Shieh-Yang-Sun's, but also enhances the security.

References

[1] S.P. Shieh, W.H. Yang, and H.M. Sun. An authentication protocol without trusted third party. *IEEE Communications Letters*, 1(3):87–89, May 1997.

[2] E. Okamoto and K. Tanaka. Identity-based information security management system for personal computer networks. *IEEE J. Select. Areas Commun.*, 7:290–294, Feb. 1989.

[3] A. Shamir. Identity based cryptosystems & signature schemes. In *Advances in Cryptology, CRYPTO'84*, pages 47–53, Lecture Notes in Computer Science, 1984.

[4] M. E. Smid and D. K. Branstad. The Data Encryption Standard: Past and Future. *Proc. of the IEEE*, 76(5):550–559, May 1988.

[5] S. Miyaguchi. The FEAL cipher family. In *Advances in Cryptology, CRYPTO'90*, pages 627–638, Lecture Notes in Computer Science, Vol. 435, August 1990.